Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes

Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes

Dr. Jeannette Wing

Assistant Director for Computer & Information Science and Engineering (CISE), National Science Foundation (NSF)

Dr. Carl Landwehr

Program Director, Trustworthy Computing Program, National Science Foundation (NSF)

Dr. Patricia Muoio

Science and Technology Lead for Cyber, Office of the Director of National Intelligence (ODNI)

Dr. Douglas Maughan

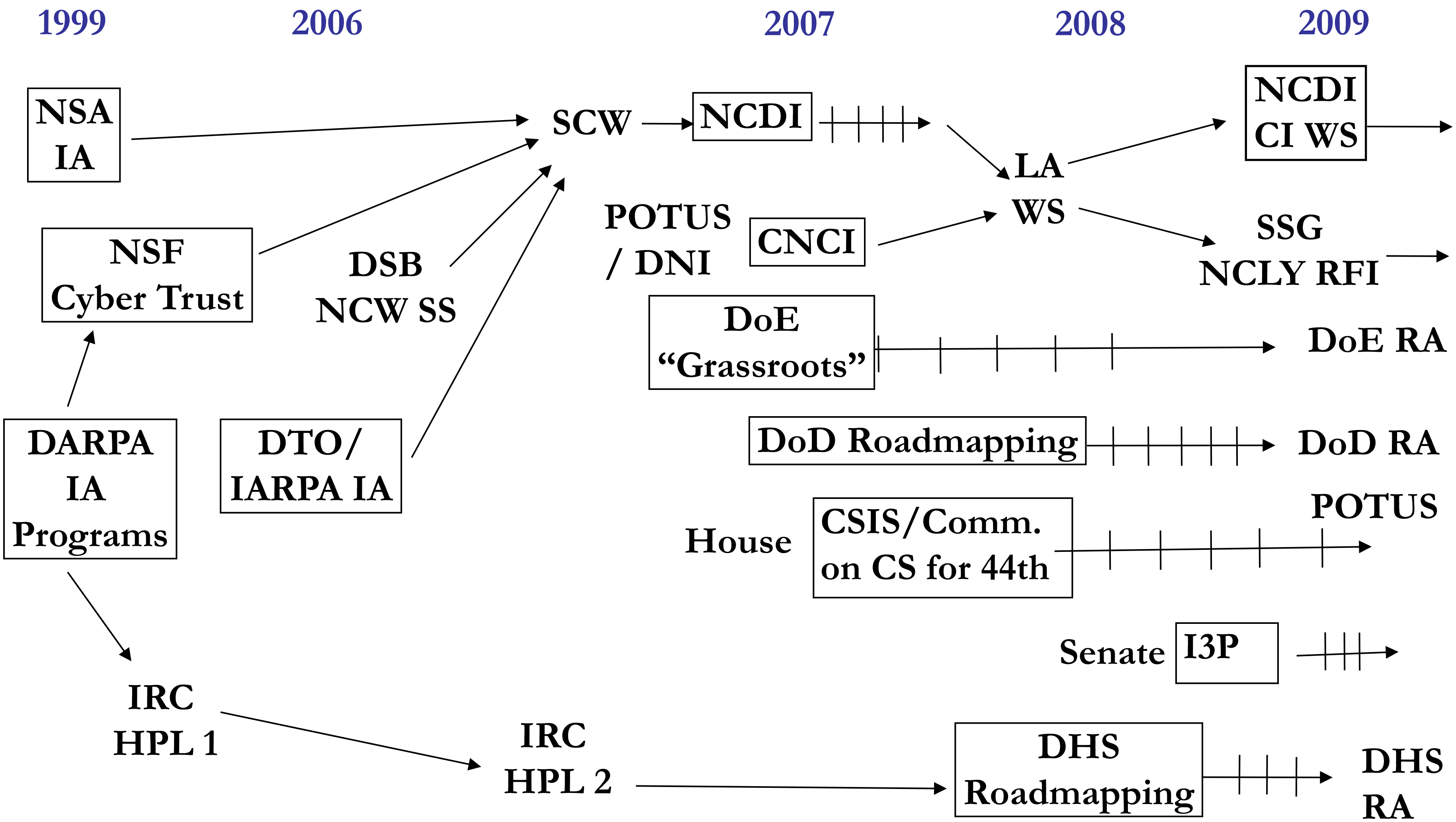
Program Manager, Cyber Security R&D, Science & Technology Directorate, Department of Homeland Security (DHS S&T)

Presented by Federal NITRD Program

May 19, 2010

Claremont Hotel
41 Tunnel Road
Berkeley, California

Federal Cybersecurity R&D: National Dialogue



1999

2006

2007

2008

2009

NSA IA

NSF Cyber Trust

DARPA IA Programs

DSB NCW SS

DTO/ IARPA IA

SCW

NCDI

POTUS / DNI

CNCI

DoE "Grassroots"

DoD Roadmapping

House

CSIS/Comm. on CS for 44th

Senate

I3P

LA WS

NCDI CI WS

SSG NCLY RFI

DoE RA

DoD RA

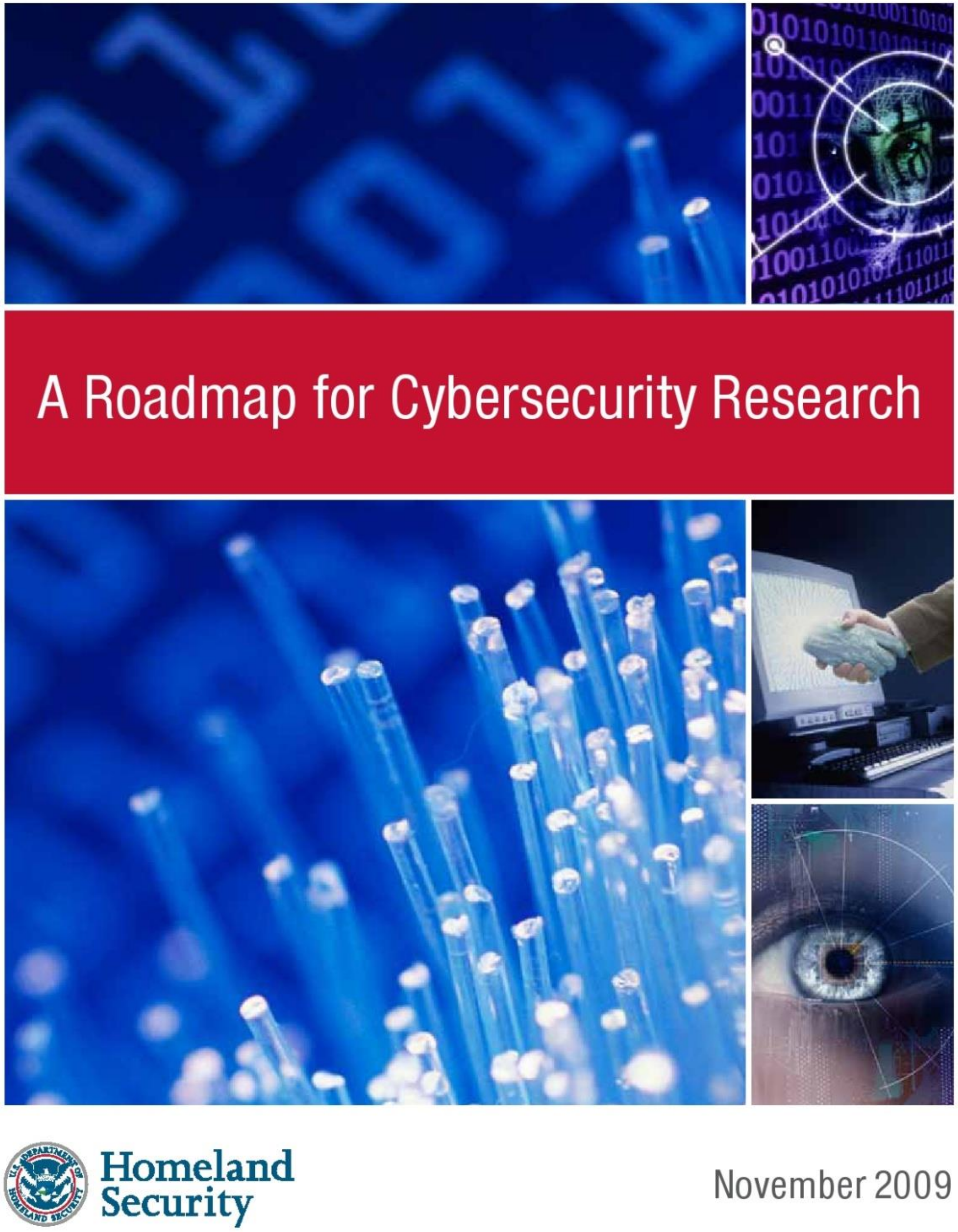
POTUS

IRC HPL 1

IRC HPL 2

DHS Roadmapping

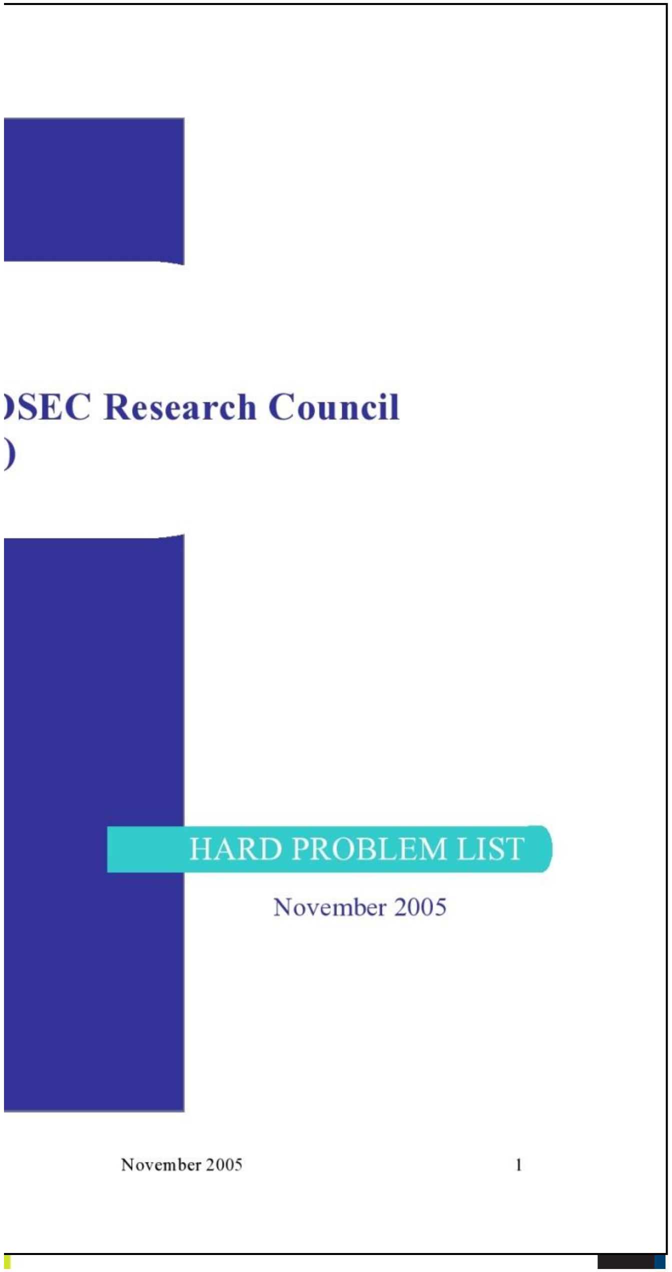
DHS RA



A Roadmap for Cybersecurity Research

Homeland Security

November 2009



SEC Research Council
)

HARD PROBLEM LIST

November 2005

November 2005 1

Say “No!” to Business as Usual

Coordinated Effort on Game-Changers

- It’s about trustworthiness of digital infrastructure
  - Security, reliability, resiliency, privacy, usability
  - How can we:
    - Enable risk-aware safe operations in co
    - Minimize critical system risk while incr exposure
    - Support informed trust decisions, necess strategies, and allowing for effective risk/bene implementations

“Locution for radical thinking”
[P. Muoio]

- Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda
  - Comprehensive National Cybersecurity Initiative, Cyberspace Policy Review: http://www.whitehouse.gov/cybersecurity
  - Aneesh Chopra, US Chief Technology Officer
  - Howard Schmidt, President’s Cybersecurity Coordinator
  - NITRD Senior Steering Group, Interagency WGs CSIA, …

Three Themes

- Tailored trustworthy spaces
  - Supporting context specific trust decisions
- Moving target
  - Providing resilience through agility
- Cyber economics
  - Providing incentives to good security

Remember: These are just starting points.

Tailored Trustworthy Spaces

Game Changing Theme

Carl E. Landwehr

National Science Foundation

Program Director

Trustworthy Computing Program

What is a Tailored Trustworthy Space?

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor’s office, bank, theatre

- Different behaviors and controls are appropriate in different spaces

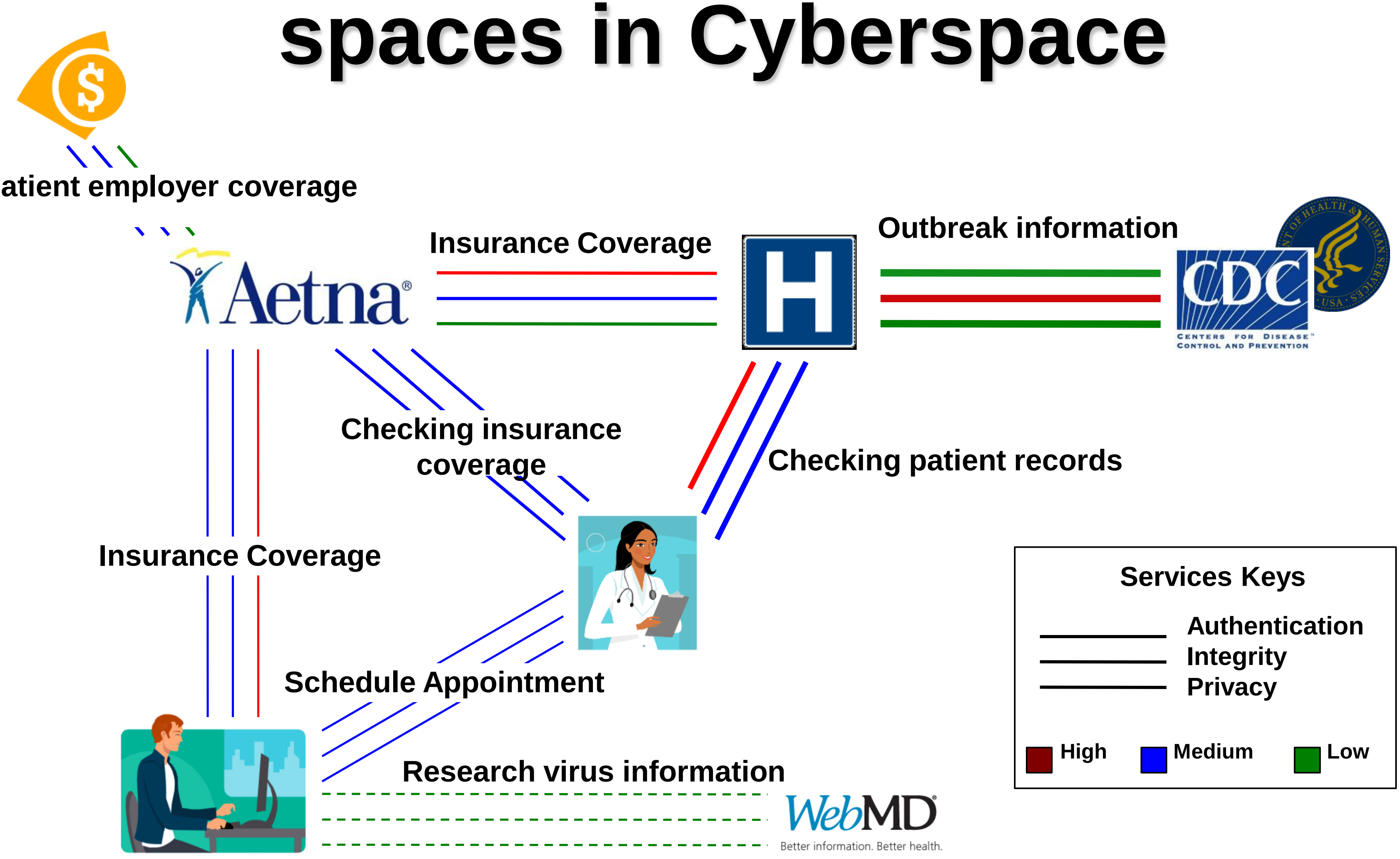
Today’s cyberspace recreates those environments, but blurs the boundaries -- sometimes merges them

The vision is of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

New Paradigm

- Users can select different environments for different activities (e.g., online banking, commerce, healthcare, personal communications) providing operating capabilities across many dimensions, including confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to create new environments with mutually agreed characteristics and lifetimes

EXAMPLE: Healthcare sub-spaces in Cyberspace



Patient employer coverage

Insurance Coverage

Outbreak information

Checking insurance coverage

Checking patient records

Insurance Coverage

Schedule Appointment

Research virus information

Services Keys

Authentication
Integrity
Privacy

🟥 High 🟦 Medium 🟩 Low

Aetna
CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION
WebMD
Better information. Better health.

Enabling Informed Trust Decisions

- Provide users with:
  - Context-specific trust services
  - Coherent policy implementation: an integrated set of security choices (or defaults) appropriate to the tasks at hand
  - User/provider/system visible rules and attributes
  - Means to negotiate boundaries and rules of the space

Challenge: Identifying dimensions of a tailored trustworthy space

- Degree of identification / authentication
- Information flow rules
- Strength of separation mechanisms
- Degree of monitoring / violation detection

Challenge: Policy Specification and Management

- Convenient specification of a tailored space
- Convenient mechanisms to know it
- Convenient mechanisms to change it

- Challenge: Validation of platform integrity
- Challenge: Violation detection
- Challenge: Verifiable separation of spaces
- . . . and many more

What’s New?

Nothing. Few of these individual problems or component technologies are novel

Everything. A structure that puts the pieces together to provide integrated, usable support for diverse trust environments would change the game.

Which technology areas matter?

- Identity management
- Component assurance
- Composition methods and logics
- Trust negotiation and management
- ...

Moving Target

Game Changing Theme

Patricia A. Muoio

ODNI Science and Technology Lead for Cyber

What is Moving Target

- Controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

New Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- Cybersecurity is an adversarial science

Seizing the Advantage

By establishing controlled movement across multiple system dimensions, we can shift the advantage to the defender by increasing:

- The costs to an attacker in time and resources for reconnaissance, planning, and development
  - the degrees of uncertainty for the attacker
  - the apparent complexity of an individual target
  - the apparent diversity across any set of targets
- The range of defense strategies available to the defender
- The resiliency and fault tolerance of the target through redundant paths, resources, and configurations

Challenge: Managing Moving Target Systems

- Moving target systems should confound the adversary, not the user
  - Need system management and configuration capabilities that can support correct use of highly complex systems
  - Need cognitive interfaces to moving target systems
- Deployment of moving target mechanisms requires complex cost/benefit analysis
  - Need metrics and analytic methods to enable such analysis
- Each moving target mechanism addresses only a subset of the attack vectors
  - Need decision support mechanism for deployment of moving target systems

Challenge: Smart Movement

- Moving targets need to be agile
  - We need to consider autonomic behavior and concepts learned from analysis of immune systems, species evolution, and other natural responses to threat
- Moving target mechanisms need to adapt quickly
  - We need to get within the adversaries re-design loop
- Moving target mechanisms have performance costs
  - We need system control mechanisms that enable real-time threat-appropriate selection of moving target protections

Challenge: Developing a Cyber Ecosystem to Support Agility

- Keyed random moving target systems present key management challenges
  - Need systems that accommodate ad hoc key distribution, rapid re-keying
- Moving target mechanisms require complex decisions
  - Need enhanced capabilities to provide situational awareness of system state and current threats
  - Need metrics to support both human and machine decision making
- Moving target at scale may result in highly complex systems
  - Need new methods to model, test and evaluate such systems

Cyber Economic Incentives

Game Changing Theme

W. Douglas Maughan

DHS Science and Technology (S&T)
Program Manager

What is Cyber Economic Incentives?

- An examination to determine what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - New theories and models of investments, markets, and the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models and support for “personal data ownership”

What needs to change?

- Promotion of science-based understanding of markets, decision-making and investment motivation
  - Develop new theories and models
  - Promote the role of economics as part of that understanding
- Creation of environments where deployment of security technology is balanced
  - Incentives to engage in socially responsible behavior
  - Deterrence for those who participate in criminal and malicious behavior

Challenge: Cyberspace Data

- Legal and ethical collection, protection and distribution
  - Ensure *all* data types/categories are available to the R&D community, including international sharing
  - Provide protections to data providers, e.g., anonymization
- Lack of appropriate data to support effective economic analysis
  - Why isn’t there cyber “insurance actuarial information”?
  - Current incident trending information inadequate for decision-makers (e.g., no “ground truth” for malware, incidents, etc.)

Challenge: Personal Info/Behavior

- Educating users about the benefits of secure practices and acceptable cyber behavior
  - Currently, the “user” is the weakest link
  - Will improved usability impact the security deployment picture?
- “Personal Data”
  - Lack of understanding and agreement of what it is
  - Who’s ultimately responsible for *my* personal data? Can I hold them accountable? Do I actually *own* it? What economic issues are associated with “personal data”?

Challenge: Empowerment of critical infrastructure providers

- Assess economic benefits and costs of protecting critical infrastructure against disruption
  - Educate vendors about their role w.r.t. “secure” software
- Provide legal frameworks allowing service providers to be more active in defense of their systems/services
  - What is allowable scope of action in “active response”, within the context of global legal capacities and partnerships?
  - How do we empower providers to reduce abusive or criminal behavior and provide appropriate law enforcement support?

What is the end result?

- Data for everyone, anytime, anywhere
- Security deployment decisions based on knowledge, metrics, and proper motivations
- Properly incentivized vendors
- Individual users taking ownership of their personal data
- Critical infrastructure providers able to better defend their networks and systems

Why Should You Care?

How Can You Get Involved?

We Want Your Input and Comments

Federal R&D agencies will use your input to refine the R&D themes, to structure research activities, and to provide the basis for requests for additional Federal research funding

Contribute ideas

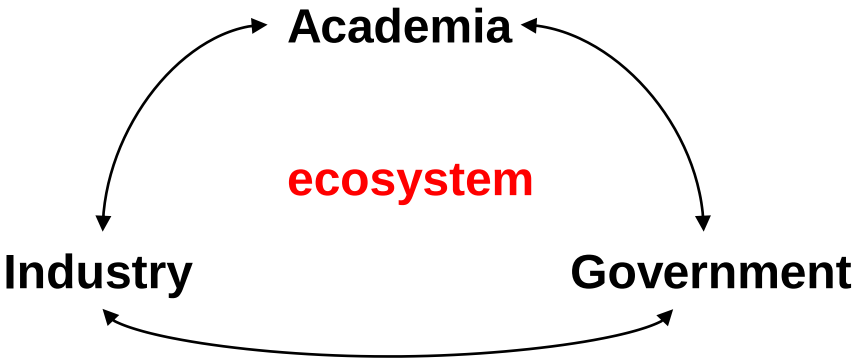
Share results

Public Comment Period (5/19-6/18, 2010)

- Visit: http://cybersecurity.nitrd.gov to share your comments and participate in the Forum
- Email to: cybersecurity@nitrd.gov
- Mail to: NCO/NITRD, Suite II-405, 4201 Wilson Boulevard, Arlington, Virginia 22230

It’s a Collective Effort: Examples

- Shared datasets
- Red Teaming
- System stress tests
- Shared common problem to tackle
- …



- New models of engagement
- *Sustained* investment models
- Lightweight submission and reporting
- …

Think Big, Think Novel

It’s about making our nation more cybersecure, not about the quest for the next 12-month, 12-page chunk of work.*

*J.M.Wing, CACM Blog Entry “Breaking the Cycle”, August 2009.
http://cacm.acm.org/blogs/blog-cacm/38402-breaking-the-cycle/fulltext